(19)日本国特許庁（ＪＰ）　(12) **公開特許公報**（Ａ）　(11)特許出願公開番号
特開2000－89668
（P2000－89668A）
(43)公開日　平成12年３月31日(2000.3.31)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）
Ｇ０９Ｃ　1/00	６２０	Ｇ０９Ｃ　1/00	６２０Ｚ	

審査請求　未請求　請求項の数12　ＯＬ　（全 10 頁）

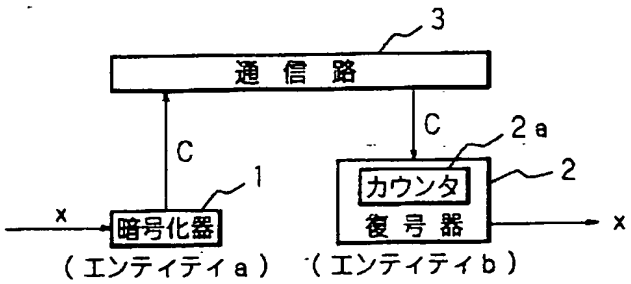
(21)出願番号　特願平10－262036

(22)出願日　平成10年９月16日(1998.9.16)

(71)出願人　000006297
村田機械株式会社
京都府京都市南区吉祥院南落合町３番地
(71)出願人　597008636
笠原　正雄
大阪府箕面市粟生外院４丁目15番３号
(72)発明者　笠原　正雄
大阪府箕面市粟生外院４丁目15番３号
(72)発明者　村上　恭通
京都府京都市伏見区竹田向代町136番地
村田機械株式会社本社工場内
(74)代理人　100078868
弁理士　河野　登夫

(54)【発明の名称】　暗号化方法，復号方法，暗号化・復号方法及び暗号通信システム

(57)【要約】
【課題】　高速の復号が可能な積和型暗号の暗号化・復号方法を提供する。
【解決手段】　平文ベクトルm＝（m_0，m_1，…，m_{K-1}）と基数ベクトルB＝（B_0，B_1，…，B_{K-1}）とを用いた内積により暗号文C＝$m_0 B_0 + m_1 B_1 + \cdots + m_{K-1} B_{K-1}$を得る積和型の暗号方式であって、$B_i$（$0 \leqq i \leqq K-1$）を$B_i = b_0 b_1 \cdots b_i$に設定する。



【特許請求の範囲】

【請求項１】　平文をＫ分割した平文ベクトルｍ＝（m_0，m_1，…，m_{K-1}）と基数ベクトルＢ＝（B_0，B_1，…，B_{K-1}）とを用いて暗号文Ｃ＝$m_0B_0+m_1B_1+\cdots+m_{K-1}B_{K-1}$を得る暗号化方法において、前記$B_i$（$0\leqq i\leqq K-1$）を整数$b_i$を用いて$B_i=b_0\,b_1\cdots b_i$に設定することを特徴とする暗号化方法。

【請求項２】　前記Ｋは２のべき乗数である請求項１記載の暗号化方法。

【請求項３】　請求項１によって暗号化された前記暗号文Ｃを復号する復号方法であって、以下のアルゴリズムにより暗号文Ｃから平文ベクトルｍ＝（m_0，m_1，…，m_{K-1}）を求めることを特徴とする復号方法。

ステップ０

$C_0=C/b_0$

$m_0\equiv C_0 \pmod{b_1}$

ステップｉ（ｉ＝１～Ｋ－２）

$C_i=(C_{i-1}-m_{i-1})/b_i$

$m_i\equiv C_i \pmod{b_{i+1}}$

ステップＫ－１

$m_{K-1}=(C_{K-2}-m_{K-2})/b_{K-1}$

【請求項４】　平文をＫ分割した平文ベクトルｍ＝（m_0，m_1，…，m_{K-1}）と基数ベクトルＢ＝（B_0，B_1，…，B_{K-1}）とを用いて暗号文Ｃ＝$m_0B_0+m_1$＊$B_1+\cdots+m_{K-1}B_{K-1}$を得る暗号化方法において、前記$B_i$（$0\leqq i\leqq K-1$）を整数$b_i$，乱数$v_i$を用いて$B_i=v_i\,b_0\,b_1\cdots b_i$に設定することを特徴とする暗号化方法。

【請求項５】　乱数ベクトルｖ＝（v_0，v_1，…，v_{K-1}）を用いて暗号文Ｃ＝$m_0\,v_0\,B_0+m_1\,v_1\,B_1+\cdots+m_{K-1}\,v_{K-1}\,B_{K-1}$を得る請求項１記載の暗号化方法。

【請求項６】　前記Ｋ個のb_iの集合を複数組準備し、それぞれの集合毎に暗号文を得るようにした請求項１または４記載の暗号化方法。

【請求項７】　平文をＫ分割した平文ベクトルｍ＝（m_0，m_1，…，m_{K-1}）と基数ベクトルＢ＝（B_0，B_1，…，B_{K-1}）とを用いて前記平文を暗号文に変換し、その暗号文を元の平文に変換する暗号化・復号方法において、

前記B_i（$0\leqq i\leqq K-1$）を整数b_iを用いて$B_i=b_0\,b_1\cdots b_i$に設定するステップと、

ｗ＜Ｐ（Ｐ：素数）を満たすｗを選択し、式（ａ）により公開鍵ベクトルｃ＝（c_0，c_1，…，c_{K-1}）を求めるステップと、

$c_i\equiv wB_i \pmod{P}$　　…（ａ）

平文ベクトルｍと公開鍵ベクトルｃとの内積により、式（ｂ）に示す暗号文Ｃを作成するステップと、

$$C=m_0\,c_0+m_1\,c_1+\cdots+m_{K-1}\,c_{K-1}\quad\cdots(b)$$

※を有することを特徴とする暗号化・復号方法。

【請求項８】　平文をＫ（Ｋは２のべき乗数）分割した平文ベクトルｍ＝（m_0，m_1，…，m_{K-1}）と基数ベクトルＢ＝（B_0，B_1，…，B_{K-1}）とを用いて前記平文を暗号文に変換し、前記暗号文を元の平文に変換する暗号化・復号方法において、

前記B_i（$0\leqq i\leqq K-1$）を整数b_iを用いて$B_i=b_0\,b_1\cdots b_i$に設定するステップと、

ｗ＜Ｐ（Ｐ：素数）を満たすｗを選択し、式（ｄ）により公開鍵ベクトルｃ＝（c_0，c_1，…，c_{K-1}）を求めるステップと、

$c_i\equiv wB_i \pmod{P}$　　…（ｄ）

平文ベクトルｍと公開鍵ベクトルｃとの内積により、式（ｅ）に示す暗号文Ｃを作成するステップと、

$$C=m_0\,c_0+m_1\,c_1+\cdots+m_{K-1}\,c_{K-1}\quad\cdots(e)$$

第２ステップ

$MR=(M-ML)/B_{K/2}$

〔高速アルゴリズム〕ＭＬ，ＭＲに対して再び２分割アルゴリズムを適用する。４分割された中間復号文のそれぞれに再び２分割アルゴリズムを適用する。このようなことを繰り返すを有することを特徴とする暗号化・復号方法。

【請求項９】　平文をＫ分割した平文ベクトルｍ＝（m_0，m_1，…，m_{K-1}）と基数ベクトルＢ＝（B_0，Ｂ

暗号文Ｃに対して、中間復号文Ｍを式（ｃ）のようにして求めるステップと、

$M\equiv w^{-1}C \pmod{P}$　　…（ｃ）

この中間復号文Ｍを以下のアルゴリズムにより復号して平文ベクトルｍ＝（m_0，m_1，…，m_{K-1}）を求めるステップと

ステップ０

$M_0=M/b_0$

$m_0\equiv M_0 \pmod{b_1}$

ステップｉ（ｉ＝１～Ｋ－２）

$M_i=(M_{i-1}-m_{i-1})/b_i$

$m_i\equiv M_i \pmod{b_{i+1}}$

ステップＫ－１

$m_{K-1}=(M_{K-2}-m_{K-2})/b_{K-1}$

暗号文Ｃに対して、中間復号文Ｍを式（ｆ）のようにして求めるステップと、

$M\equiv w^{-1}C \pmod{P}$　　…（ｆ）

この中間復号文Ｍを以下のアルゴリズムにより復号して平文ベクトルｍ＝（m_0，m_1，…，m_{K-1}）を求めるステップと

〔２分割アルゴリズム〕

第１ステップ

$ML\equiv M \pmod{B_{K/2}}$

$_1$，…，B_{K-1}）とを用いて前記平文を暗号文に変換し、前記暗号文を元の平文に変換する暗号化・復号方法において、前記B_i（$0 \leqq i \leqq K-1$）を式（g）にて設定するステップと、

$$B_i = v_i\ b_0\ b_1 \cdots b_i \qquad \cdots (g)$$

但し、v_i：乱数

b_i：整数

$$C = m_0\ c_0 + m_1\ c_1 + \cdots + m_{K-1}\ c_{K-1} \qquad \cdots (i)$$

暗号文Cに対して、中間復号文Mを式（j）のようにして求めるステップと、

$$M \equiv w^{-1}C \pmod{P} \qquad \cdots (j)$$

この中間復号文Mを以下のアルゴリズムにより復号して平文ベクトル$m = (m_0, m_1, \cdots, m_{K-1})$を求めるステップと

ステップ0

$M_0 = C / b_0$

$m_0 \equiv M_0\ v_0^{-1} \pmod{b_1}$

ステップi（$i = 1 \sim K-2$）

$M_i = (M_{i-1} - m_{i-1}\ v_{i-1}) / b_i$

$m_i \equiv M_i\ v_i^{-1} \pmod{b_{i+1}}$

ステップK－1

$M_{K-1} = (M_{K-2} - m_{K-2}\ v_{K-2}) / b_{K-1}$

$m_{K-1} = M_{K-1} / v_{K-1}$

を有することを特徴とする暗号化・復号方法。

【請求項１０】　平文をK分割した平文ベクトル$m = (m_0, m_1, \cdots, m_{K-1})$と基数ベクトル$B =$

$$C = m_0\ c_0 + m_1\ c_1 + \cdots + m_{K-1}\ c_{K-1} \qquad \cdots (l)$$

暗号文Cに対して、法P，法Qにおいて、それぞれ中間復号文M_P，M_Qを式（m），式（n）のようにして求めるステップと、

$$M_P \equiv w^{-1}C \pmod{P} \qquad \cdots (m)$$

$$M_Q \equiv w^{-1}C \pmod{Q} \qquad \cdots (n)$$

この中間復号文M_P，M_Qを以下のアルゴリズムにより復号して平文ベクトル$m = (m_0, m_1, \cdots, m_{K-1})$を求めるステップと

ステップ0

$M_{P0} = M_P / b_{P0}$

$M_{Q0} = M_Q / b_{Q0}$

$m_0^{(P)} \equiv M_{P0} \pmod{b_{P1}}$

$m_0^{(Q)} \equiv M_{Q0} \pmod{b_{Q1}}$

中国人の剰余定理によりm_0を求める。

ステップi（$i = 1 \sim K-2$）

$M_{Pi} = (M_{Pi-1} - m_{i-1}) / b_{Pi}$

$M_{Qi} = (M_{Qi-1} - m_{i-1}) / b_{Qi}$

$m_i^{(P)} \equiv M_{Pi} \pmod{b_{Pi+1}}$

$m_i^{(Q)} \equiv M_{Qi} \pmod{b_{Qi+1}}$

中国人の剰余定理によりm_iを求める。

ステップK－1

$m_{K-1} = (M_{PK-2} - m_{K-2}) / b_{PK-1}$

または

＊$gcd(v_i, b_{i+1}) = 1$

$w < P$（P：素数）を満たすwを選択し、式（h）により公開鍵ベクトル$c = (c_0, c_1, \cdots, c_{K-1})$を求めるステップと、

$$c_i \equiv w B_i \pmod{P} \qquad \cdots (h)$$

平文ベクトルmと公開鍵ベクトルcとの内積により、式（i）に示す暗号文Cを作成するステップと、

※（B_0，B_1，…，B_{K-1}）とを用いて前記平文を暗号文に変換し、前記暗号文を元の平文に変換する暗号化・復号方法において、

素数P，Qを設定するステップと、

基数ベクトルB_{Pi}（$0 \leqq i \leqq K-1$）を整数b_{Pi}を用いて$B_{Pi} = b_{P0} b_{P1} \cdots b_{Pi}$に設定するステップと、

基数ベクトルB_{Qi}（$0 \leqq i \leqq K-1$）を整数b_{Qi}を用いて$B_{Qi} = b_{Q0} b_{Q1} \cdots b_{Qi}$に設定するステップと、

中国人の剰余定理を用いて、P，Qによる余りがそれぞれB_{Pi}，B_{Qi}となるような最小の整数B_iを導くステップと、

$w < N$（$N = PQ$）を満たすwを選択し、式（k）により公開鍵ベクトル$c = (c_0, c_1, \cdots, c_{K-1})$を求めるステップと、

$$c_i \equiv w B_i \pmod{N} \qquad \cdots (k)$$

平文ベクトルmと公開鍵ベクトルcとの内積により、式（l）に示す暗号文Cを作成するステップと、

$m_{K-1} = (M_{QK-2} - m_{K-2}) / b_{QK-1}$

を有することを特徴とする暗号化・復号方法。

【請求項１１】　前記Nを法として前記暗号文Cを送るようにした請求項１０記載の暗号化・復号方法。

【請求項１２】　複数のエンティティ間で暗号文による情報通信を行う暗号通信システムにおいて、請求項１，２，４，５または６の何れかに記載の暗号化方法を用いて平文から暗号文を作成する暗号化器と、作成した暗号文を一方のエンティティから他方のエンティティへ送信する通信路と、送信された暗号文を元の平文に復号する復号器とを備えることを特徴とする暗号通信システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、平文を暗号文に変換するための暗号化方法、及び、暗号文を元の平文に変換するための復号方法に関し、特に、積和型暗号に関する。

【０００２】

【従来の技術】高度情報化社会と呼ばれる現代社会では、コンピュータネットワークを基盤として、ビジネス上の重要な文書・画像情報が電子的な情報という形で伝送通信されて処理される。このような電子情報は、容易に複写が可能である、複写物とオリジナルとの区別が困

難であるという性質があり、情報保全の問題が重要視されている。特に、「コンピュータリソースの共有」，「マルチアクセス」，「広域化」の各要素を満たすコンピュータネットワークの実現が高度情報化社会の確立に不可欠であるが、これは当事者間の情報保全の問題とは矛盾する要素を含んでいる。このような矛盾を解消するための有効な手法として、人類の過去の歴史上主として軍事，外交面で用いられてきた暗号技術が注目されている。

【０００３】暗号とは、情報の意味が当事者以外には理解できないように情報を交換することである。暗号において、誰でも理解できる元の文（平文）を第三者には意味がわからない文（暗号文）に変換することが暗号化であり、また、暗号文を平文に戻すことが復号であり、この暗号化と復号との全過程をまとめて暗号系と呼ぶ。暗号化の過程及び復号の過程には、それぞれ暗号化鍵及び復号鍵と呼ばれる秘密の情報が用いられる。復号時には秘密の復号鍵が必要であるので、この復号鍵を知っている者のみが暗号文を復号でき、暗号化によって情報の秘密性が維持され得る。

【０００４】暗号化方式は、大別すると共通鍵暗号系と公開鍵暗号系との二つに分類できる。共通鍵暗号系では、暗号化鍵と復号鍵とが等しく、送信者と受信者とが同じ鍵を持つことによって暗号通信を行う。送信者が平文を秘密の共通鍵に基づいて暗号化して受信者に送り、受信者はこの共通鍵を用いて暗号文を元に平文に復号する。

【０００５】これに対して公開鍵暗号系では、暗号化鍵と復号鍵とが異なっており、公開されている受信者の公開鍵で送信者が平文を暗号化し、受信者が自身の秘密鍵でその暗号文を復号することによって暗号通信を行う。公開鍵は暗号化のための鍵、秘密鍵は公開鍵によって変換された暗号文を復号するための鍵であり、公開鍵によって変換された暗号文は秘密鍵でのみ復号することができる。

【０００６】

【発明が解決しようとする課題】公開鍵暗号系の１つである積和型暗号に関して、新規な方式及び攻撃法が次々に提案されているが、特に、多くの情報を短時間で処理できるように高速復号可能な暗号化・復号の手法の開発が望まれている。

【０００７】本発明は斯かる事情に鑑みてなされたものであり、多進法を用いることにより、高速な復号処理が可能である、積和型暗号における新規の暗号化方法及び復号方法を提供することを目的とする。

【０００８】

【課題を解決するための手段】請求項１に係る暗号化方法は、平文をＫ分割した平文ベクトルｍ＝（m_0，m_1，…，m_{K-1}）と基数ベクトルＢ＝（B_0，B_1，…，B_{K-1}）とを用いて暗号文Ｃ＝$m_0 B_0 + m_1 B_1 + \cdots + m_{K-1} B_{K-1}$ を得る暗号化方法において、前記B_i（$0 \leqq i \leqq K-1$）を整数b_iを用いて$B_i = b_0 b_1 \cdots b_i$に設定することを特徴とする。

【０００９】請求項２に係る暗号化方法は、請求項１において、前記Ｋは２のべき乗数であることを特徴とする。

【００１０】請求項３に係る復号方法は、請求項１によって暗号化された前記暗号文Ｃを復号する復号方法であって、以下のアルゴリズムにより暗号文Ｃから平文ベクトルｍ＝（m_0，m_1，…，m_{K-1}）を求めることを特徴とする。

ステップ０

$C_0 = C / b_0$

$m_0 \equiv C_0 \pmod{b_1}$

ステップｉ（ｉ＝１～Ｋ－２）

$C_i = (C_{i-1} - m_{i-1}) / b_i$

$m_i \equiv C_i \pmod{b_{i+1}}$

ステップＫ－１

$m_{K-1} = (C_{K-2} - m_{K-2}) / b_{K-1}$

【００１１】請求項４に係る暗号化方法は、平文をＫ分割した平文ベクトルｍ＝（m_0，m_1，…，m_{K-1}）と基数ベクトルＢ＝（B_0，B_1，…，B_{K-1}）とを用いて暗号文Ｃ＝$m_0 B_0 + m_1 B_1 + \cdots + m_{K-1} B_{K-1}$ を得る暗号化方法において、前記B_i（$0 \leqq i \leqq K-1$）を整数b_i，乱数v_iを用いて$B_i = v_i b_0 b_1 \cdots b_i$に設定することを特徴とする。

【００１２】請求項５に係る暗号化方法は、請求項１において、乱数ベクトルｖ＝（v_0，v_1，…，v_{K-1}）を用いて暗号文Ｃ＝$m_0 v_0 B_0 + m_1 v_1 B_1 + \cdots + m_{K-1} v_{K-1} B_{K-1}$ を得ることを特徴とする。

【００１３】請求項６に係る暗号化方法は、請求項１または４において、前記Ｋ個のb_iの集合を複数組準備し、それぞれの集合毎に暗号文を得るようにしたことを特徴とする。

【００１４】請求項７に係る暗号化・復号方法は、平文をＫ分割した平文ベクトルｍ＝（m_0，m_1，…，m_{K-1}）と基数ベクトルＢ＝（B_0，B_1，…，B_{K-1}）とを用いて前記平文を暗号文に変換し、その暗号文を元の平文に変換する暗号化・復号方法において、前記B_i（$0 \leqq i \leqq K-1$）を整数b_iを用いて$B_i = b_0 b_1 \cdots b_i$に設定するステップと、ｗ＜Ｐ（Ｐ：素数）を満たすｗを選択し、式（ａ）により公開鍵ベクトルｃ＝（c_0，c_1，…，c_{K-1}）を求めるステップと、

$c_i \equiv w B_i \pmod{P}$ …（ａ）

平文ベクトルｍと公開鍵ベクトルｃとの内積により、式（ｂ）に示す暗号文Ｃを作成するステップと、

$C = m_0 c_0 + m_1 c_1 + \cdots + m_{K-1} c_{K-1}$ …（ｂ）

暗号文Ｃに対して、中間復号文Ｍを式（ｃ）のようにして求めるステップと、

$M \equiv w^{-1}C \pmod{P}$ …（c）

この中間復号文Mを以下のアルゴリズムにより復号して平文ベクトルm＝（m_0，m_1，…，m_{K-1}）を求めるステップと

ステップ0

$M_0 = M / b_0$

$m_0 \equiv M_0 \pmod{b_1}$

ステップi（i＝1～K－2）

$M_i = (M_{i-1} - m_{i-1}) / b_i$

$m_i \equiv M_i \pmod{b_{i+1}}$

ステップK－1

$m_{K-1} = (M_{K-2} - m_{K-2}) / b_{K-1}$

を有することを特徴とする。

$$C = m_0 c_0 + m_1 c_1 + \cdots + m_{K-1} c_{K-1} \quad \cdots (e)$$

暗号文Cに対して、中間復号文Mを式（f）のようにして求めるステップと、

$M \equiv w^{-1}C \pmod{P}$ …（f）

この中間復号文Mを以下のアルゴリズムにより復号して平文ベクトルm＝（m_0，m_1，…，m_{K-1}）を求めるステップと

〔２分割アルゴリズム〕

第１ステップ

$ML \equiv M \pmod{B_{K/2}}$

第２ステップ

$MR = (M - ML) / B_{K/2}$

〔高速アルゴリズム〕ML，MR に対して再び２分割アルゴリズムを適用する。４分割された中間復号文のそれぞれに再び２分割アルゴリズムを適用する。このようなことを繰り返すを有することを特徴とする。

【００１６】請求項９に係る暗号化・復号方法は、平文

$$C = m_0 c_0 + m_1 c_1 + \cdots + m_{K-1} c_{K-1} \quad \cdots (i)$$

暗号文Cに対して、中間復号文Mを式（j）のようにして求めるステップと、

$M \equiv w^{-1}C \pmod{P}$ …（j）

この中間復号文Mを以下のアルゴリズムにより復号して平文ベクトルm＝（m_0，m_1，…，m_{K-1}）を求めるステップと

ステップ0

$M_0 = C / b_0$

$m_0 \equiv M_0 v_0^{-1} \pmod{b_1}$

ステップi（i＝1～K－2）

$M_i = (M_{i-1} - m_{i-1} v_{i-1}) / b_i$

$m_i \equiv M_i v_i^{-1} \pmod{b_{i+1}}$

ステップK－1

$M_{K-1} = (M_{K-2} - m_{K-2} v_{K-2}) / b_{K-1}$

$m_{K-1} = M_{K-1} / v_{K-1}$

を有することを特徴とする。

【００１７】請求項10に係る暗号化方法・復号方法は、

$$C = m_0 c_0 + m_1 c_1 + \cdots + m_{K-1} c_{K-1} \quad \cdots (l)$$

暗号文Cに対して、法P，法Qにおいて、それぞれ中間

＊【００１５】請求項８に係る暗号化方法・復号方法は、平文をK（Kは２のべき乗数）分割した平文ベクトルm＝（m_0，m_1，…，m_{K-1}）と基数ベクトルB＝（B_0，B_1，…，B_{K-1}）とを用いて前記平文を暗号文に変換し、前記暗号文を元の平文に変換する暗号化・復号方法において、前記B_i（0≦i≦K－1）を整数b_iを用いて$B_i = b_0 b_1 \cdots b_i$に設定するステップと、w＜P（P：素数）を満たすwを選択し、式（d）により公開鍵ベクトルc＝（c_0，c_1，…，c_{K-1}）を求めるステップと、

$c_i \equiv w B_i \pmod{P}$ …（d）

平文ベクトルmと公開鍵ベクトルcとの内積により、式（e）に示す暗号文Cを作成するステップと、

※をK分割した平文ベクトルm＝（m_0，m_1，…，m_{K-1}）と基数ベクトルB＝（B_0，B_1，…，B_{K-1}）とを用いて前記平文を暗号文に変換し、前記暗号文を元の平文に変換する暗号化・復号方法において、前記B_i（0≦i≦K－1）を式（g）にて設定するステップと、

$B_i = v_i b_0 b_1 \cdots b_i$ …（g）

但し、v_i：乱数

b_i：整数

$gcd(v_i, b_{i+1}) = 1$

w＜P（P：素数）を満たすwを選択し、式（h）により公開鍵ベクトルc＝（c_0，c_1，…，c_{K-1}）を求めるステップと、

$c_i \equiv w B_i \pmod{P}$ …（h）

平文ベクトルmと公開鍵ベクトルcとの内積により、式（i）に示す暗号文Cを作成するステップと、

★平文をK分割した平文ベクトルm＝（m_0，m_1，…，m_{K-1}）と基数ベクトルB＝（B_0，B_1，…，B_{K-1}）とを用いて前記平文を暗号文に変換し、前記暗号文を元の平文に変換する暗号化・復号方法において、素数P，Qを設定するステップと、基数ベクトルB_{Pi}（0≦i≦K－1）を整数b_{Pi}を用いて$B_{Pi} = b_{P0} b_{P1} \cdots b_{Pi}$に設定するステップと、基数ベクトル$B_{Qi}$（0≦i≦K－1）を整数$b_{Qi}$を用いて$B_{Qi} = b_{Q0} b_{Q1} \cdots b_{Qi}$に設定するステップと、中国人の剰余定理を用いて、P，Qによる余りがそれぞれB_{Pi}，B_{Qi}となるような最小の整数B_iを導くステップと、w＜N（N＝PQ）を満たすwを選択し、式（k）により公開鍵ベクトルc＝（c_0，c_1，…，c_{K-1}）を求めるステップと、

$c_i \equiv w B_i \pmod{N}$ …（k）

平文ベクトルmと公開鍵ベクトルcとの内積により、式（l）に示す暗号文Cを作成するステップと、

復号文M_P，M_Qを式（m），式（n）のようにして求

めるステップと、

$M_P \equiv w^{-1}C \pmod{P}$ … (m)

$M_Q \equiv w^{-1}C \pmod{Q}$ … (n)

この中間復号文M_P，M_Qを以下のアルゴリズムにより復号して平文ベクトル$m=(m_0, m_1, \cdots, m_{K-1})$を求めるステップと

ステップ0

$M_{P0}=M_P / b_{P0}$

$M_{Q0}=M_Q / b_{Q0}$

$m_0^{(P)} \equiv M_{P0} \pmod{b_{P1}}$

$m_0^{(Q)} \equiv M_{Q0} \pmod{b_{Q1}}$

中国人の剰余定理によりm_0を求める。

ステップi（i＝1～K－2）

$M_{Pi}=(M_{Pi-1}-m_{i-1}) / b_{Pi}$

$M_{Qi}=(M_{Qi-1}-m_{i-1}) / b_{Qi}$

$m_i^{(P)} \equiv M_{Pi} \pmod{b_{Pi+1}}$

$m_i^{(Q)} \equiv M_{Qi} \pmod{b_{Qi+1}}$

中国人の剰余定理によりm_iを求める。

ステップK－1

$m_{K-1}=(M_{PK-2}-m_{K-2}) / b_{PK-1}$

または

$*m_{K-1}=(M_{QK-2}-m_{K-2}) / b_{QK-1}$

を有することを特徴とする。

【００１８】請求項11に係る暗号化・復号方法は、請求項10において、前記Ｎを法として前記暗号文Ｃを送るようにしたことを特徴とする。

【００１９】請求項12に係る暗号通信システムは、複数のエンティティ間で暗号文による情報通信を行う暗号通信システムにおいて、請求項１，２，４，５または６の何れかに記載の暗号化方法を用いて平文から暗号文を作成する暗号化器と、作成した暗号文を一方のエンティティから他方のエンティティへ送信する通信路と、送信された暗号文を元の平文に復号する復号器とを備えることを特徴とする。

【００２０】本発明の暗号化方法・復号方法の概念について、以下に説明する。本発明では、多進法を用いる。

【００２１】メッセージ$m=(m_0, m_1, \cdots, m_{K-1})$を基数$B=(B_0, B_1, \cdots, B_{K-1})$を用いて、下記式（１）に示すように、整数として表記することができる。なお、ここでは、$m_i B_i < B_{i+1}$が成立するものとする。

$$M=m_0 B_0+m_1 B_1+\cdots+m_{K-1} B_{K-1} \quad \cdots (1)$$

なお、このアルゴリズムにあっては、$m_j < b_{j+1}$でないと、m_jが一意に復号されない。

【００２７】このような多進法による暗号化手法とそれに対する復号方法とを、本発明の特徴とする。なお、具体的な手法については後述する。

【００２８】

【発明の実施の形態】以下、本発明の実施の形態について具体的に説明する。図１は、本発明による暗号化方法・復号方法をエンティティａ，ｂ間の情報通信に利用した状態を示す模式図である。図１の例では、一方のエンティティａが、暗号化器１にて平文ｘを暗号文Ｃに暗号化し、通信路３を介してその暗号文Ｃを他方のエンティティｂへ送信し、エンティティｂが、復号器２にてその暗号文Ｃを元の平文ｘに復号する場合を示している。なお、復号器２には、後述する復号処理時に利用されるカウンタ2aが内蔵されている。

【００２９】（第１実施の形態）秘密鍵と公開鍵とを以下のように準備する。

・秘密鍵：$\{b_i\}$，Ｐ，ｗ

・公開鍵：$\{c_i\}$

前記式（２）のように基数を与え、ｗ＜Ｐ（Ｐは大きな素数）を満たす整数ｗをランダムに選び、式（３）を導く。

$c_i \equiv w B_i \pmod{P}$ … (3)

公開鍵ベクトルｃは、式（４）のように与えられる。

$c=(c_0, c_1, \cdots, c_{K-1})$ … (4)

【００３０】また、$\mu < min(b_1, \cdots, b_{K-1})$なる$\mu$が各エンティティに公開される。エンティティａ側

$M=m_0 B_0+m_1 B_1+\cdots+m_{K-1} B_{K-1}$ … (1)

【００２２】式（１）において、$B_i=2^i$である場合にはメッセージは通常の２進数で表されていることになり、$B_i=10^i$である場合にはメッセージは通常の10進数で表されていることになる。

【００２３】ここで、上記B_iを下記式（２）のように設定する場合を考える。

$B_i=b_0 b_1 \cdots b_i$ … (2)

式（２）において、$b_0=1$，$b_i=2$（$1 \leqq i \leqq K-1$）と設定すると２進数の場合に一致し、$b_0=1$，$b_i=10$（$1 \leqq i \leqq K-1$）と設定すると10進数の場合に一致する。

【００２４】本発明では、このような多進法を用い、つまり、式（１）及び式（２）を利用して、暗号文を作成する。

【００２５】そして、基数を式（２）で与えた場合には、以下に示すアルゴリズムにより、整数Ｍからメッセージ$m=(m_0, m_1, \cdots, m_{K-1})$を復号することができる。この復号アルゴリズムを逐次復号アルゴリズムＩという。

【００２６】〔逐次復号アルゴリズムＩ〕

ステップ0

$M_0=M/b_0$

$m_0 \equiv M_0 \pmod{b_1}$

ステップi（i＝1～K－2）

$M_i=(M_{i-1}-m_{i-1}) / b_i$

$m_i \equiv M_i \pmod{b_{i+1}}$

ステップK－1

$m_{K-1}=(M_{K-2}-m_{K-2}) / b_{K-1}$

で、この公開されたμに基づいて、K次元のμ以下の大きさのメッセージベクトルに平文xを分割する。このようにメッセージのビット数を制限すると、b_0，b_1，…，b_{K-1} の大小関係は任意に設定して良い。そして、＊

$$C=m_0 c_0+m_1 c_1+\cdots+m_{K-1} c_{K-1} \quad \cdots(5)$$

【００３１】なお、この暗号化は、K重の並列処理による乗算１回、更に $\log_2 K$ 回の加算処理の所要時間で行える。

【００３２】エンティティｂ側では、以下のようにして復号処理が行われる。暗号文Cに対して、中間復号文M※

$$M=m_0 b_0+m_1 b_0 b_1+\cdots+m_{K-1} b_0 b_1 \cdots b_{K-1} \quad \cdots(7)$$

【００３３】図２は、復号器２で行われるこの逐次復号アルゴリズムＩの処理手順を示すフローチャートである。まず、カウンタ2aをリセットして、そのカウント値Tを０にする（Ｓ１）。そして、ステップ０の演算を実行してm_0を求めた後（Ｓ２）、カウント値Tを１にする（Ｓ３）。次に、ステップｉを実行してm_iを求め（Ｓ４）、カウント値Tを１だけインクリメントする（Ｓ５）。カウント値TがＫ－１に達したか否かを判断し（Ｓ６）、達していない場合には（Ｓ６：ＮＯ）、Ｓ★

$$w b_0 b_1 \cdots b_J / w b_0 b_1 \cdots b_{J-1} \equiv B_J / B_{J-1} \pmod P \quad \cdots(8)$$

$$w b_0 b_1 \cdots b_{J+1} / w b_0 b_1 \cdots b_J \equiv B_{J+1} / B_J \pmod P \quad \cdots(9)$$

$$(B_J)^2 - B_{J-1} B_J = Ng \quad \cdots(10)$$

一方、b_i を p^d の周辺でランダムに選んだ場合、１つのb_i の値を総当たり的に仮定することにより、やはりPが露呈する。b_i は64ビット程度以上に選ぶ必要がある。

【００３５】この第１実施の形態は、０，１ナップザック暗号を一般化した手法として位置づけることもできる。即ち、$m_i \in GF(2)$ とすれば、超増加数列 $\{b_0, b_0 b_1, \cdots, b_0 b_1 \cdots b_{K-1}\}$ による０，１ナップザック暗号に一致する。

【００３６】一般に超増加数列を用いた従来の積和型暗号方式では、基数相互間に関係がなく、平文の上位桁か☆

＊そのメッセージベクトルmと公開鍵ベクトルｃとの内積を式（５）のように求めて、平文xを暗号化して暗号文Ｃを得る。作成された暗号文Ｃは通信路３を介してエンティティａからエンティティｂへ送信される。

※を式（６）のようにして求める。

$$M \equiv w^{-1} C \pmod P \quad \cdots(6)$$

この中間復号文Mは、具体的には式（７）として与えられるので、前述の逐次復号アルゴリズムＩによって復号できる。

★４，Ｓ５の処理を繰り返す。Ｔ＝１からＴ＝Ｋ－２までこの処理を繰り返すことによって、m_1 からm_{K-2} までが求まる。カウント値TがＫ－１に達した場合には、（Ｓ６：ＹＥＳ）、ステップＫ－１を実行してm_{K-1} を求める（Ｓ７）。

【００３４】ところで、この第１実施の形態において、b_i が $b_i = p^d$ というような単純な形である場合には、下記式（８），式（９）となるので、式（10）が成立してPが露呈することになる。

☆ら逐次復号していく必要があり、多倍長の整数を除数とする除算が必要であった。しかしながら、このb_i 進数を用いた本発明の方式では、下位桁から小さい整数を法とする剰余演算及び除算を繰り返せるので、高速に復号できることが分かる。

【００３７】復号の更なる高速化を図れる復号手法について、以下に説明する。中間復号文Mの前半部分をML、中間復号文Mの後半部分を$B_{K/2}$ で割ったものをMRとする。これらのML 及びMR は具体的には、式（11）及び式（12）で示される。なお、Kは２のべき乗数とする。

$$ML = m_0 B_0 + \cdots + m_{K/2-1} B_{K/2-1} \quad \cdots(11)$$

$$MR = (m_{K/2} B_{K/2} + \cdots + m_{K-1} B_{K-1}) / B_{K/2} \quad \cdots(12)$$

【００３８】このような２分割アルゴリズムと、それを繰り返し適用した高速アルゴリズムとを以下に示す。

【００３９】〔２分割アルゴリズム〕

第１ステップ

$ML \equiv M \pmod{B_{K/2}}$

第２ステップ

$MR = (M - ML) / B_{K/2}$

【００４０】〔高速アルゴリズム〕ML，MR に対して再び２分割アルゴリズムを適用する。４分割されたメッセージのそれぞれに再び２分割アルゴリズムを適用する。このようなことを繰り返す。

【００４１】このようにして、Kが２のべき乗である場合には、特に高速な復号処理を実現でき、この高速アルゴリズムを適用すると、前述の逐次復号アルゴリズムと比べて、$K/\log_2 K$ 倍だけ高速に復号できる。

【００４２】例えば、b_i を64ビット程度の素数とし、Ｋ＝64に選んだ場合に、暗号文Ｃの大きさは4166ビットとなるが、高速アルゴリズムによる復号時間は、$64 = 2^6$ であるので、Ｋ＝６の場合での逐次復号アルゴリズムによる復号時間とほぼ同程度となる。即ち、約10倍高速な復号処理を行える。なお、この場合、公開鍵サイズは１キロビット程度であってかなり大きいが、１ギガビット／cm^2 の高密度記録が可能となるような状況を考えると、この公開鍵サイズは実用上問題ないと言える。

【００４３】（第２実施の形態）第１実施の形態に乱数を付加した第２実施の形態について説明する。第１実施の形態では、$\{B_i\}$ が超増加数列になる。よって、超増加数列に対する攻撃法として有名なＬＬＬ（Lenatra-

Lenatra-Lovasz）法による攻撃を、第１実施の形態は受け易いという可能性がある。そこで、第２実施の形態では、基数に乱数を付加する、つまり、第１実施の形態での基数ベクトルに乱数を掛け合わせたものを基数ベクトルとして使用することによって、安全性を強化する。

【００４４】秘密鍵と公開鍵とを以下のように準備する。

・秘密鍵：｛b_i｝，｛v_i｝，Ｐ，ｗ

・公開鍵：｛c_i｝

基数B_iを式（13）のように与える。

$$B_i = v_i\ b_0\ b_1 \cdots b_i \qquad \cdots (13)$$

ここで、式（13）で示される各B_iがほぼ同じ大きさになるようにv_iを設定する。よって、｛B_i｝は超増加数列ではなくＬＬＬ法の攻撃を受けにくい。但し、ｇｃｄ（v_i，b_{i+1}）＝１を満たすものとする。

＊【００４５】整数ｗを用いて、第１実施の形態と同様に、公開鍵ベクトルｃを以下の式（14），式（15）のように求める。

$$c_i \equiv w B_i \pmod P \qquad \cdots (14)$$

$$c = (c_0, c_1, \cdots, c_{K-1}) \qquad \cdots (15)$$

【００４６】メッセージベクトルｍと公開鍵ベクトルｃとの内積により、第１実施の形態と同様に（前記式（５））、暗号文Ｃを得る。

【００４７】復号処理は、以下のようにして行われる。暗号文Ｃに対して、中間復号文Ｍを式（16）のようにして求める。

$$M \equiv w^{-1} C \pmod P \qquad \cdots (16)$$

この中間復号文Ｍは、具体的には式（17）として与えられるので、以下に示す逐次復号アルゴリズムIIによって復号できる。

$$M = m_0\ v_0\ b_0 + m_1\ v_1\ b_0\ b_1 + \cdots + m_{K-1}\ v_{K-1}\ b_0\ b_1 \cdots b_{K-1} \qquad \cdots (17)$$

【００４８】〔逐次復号アルゴリズムII〕

ステップ０

$M_0 = M / b_0$

$m_0 \equiv M_0\ v_0^{-1} \pmod{b_1}$

ステップｉ（ｉ＝１～Ｋ－２）

$M_i = (M_{i-1} - m_{i-1}\ v_{i-1}) / b_i$

$m_i \equiv M_i\ v_i^{-1} \pmod{b_{i+1}}$

ステップＫ－１

$M_{K-1} = (M_{K-2} - m_{K-2}\ v_{K-2}) / b_{K-1}$

$m_{K-1} = M_{K-1} / v_{K-1}$ ・・・・

【００４９】なお、この逐次復号アルゴリズムIIを復号器２で実行するフローチャートは、逐次復号アルゴリズムＩのフローチャート（第２図）と同様である。

【００５０】ここで、第２実施の形態における具体例を示す。

・秘密鍵

ｂ＝（１，１１，１３）

ｖ＝（１００９，１３１，７）

Ｂ＝（１００９，１４４１，１００１）

Ｐ＝２７４８１

ｗ＝７３９

$w^{-1} \equiv 702 \pmod P$

（$b_1 < b_2 < b_3$であるので、$v_1 > v_2 > v_3$と設定することにより、B_1，B_2，B_3が超増加数列にならないようにしている）

・公開鍵

$c \equiv wB$

$\equiv (3664, 20621, 25233) \pmod P$

・暗号化

メッセージをｍ＝（６，７，８）とする。

$C = c \cdot m$

$= 6 \times 3664 + 7 \times 20621 + 8 \times 25233$

$= 368195$

・復号

中間復号文Ｍを求め、逐次復号アルゴリズムIIを用いて復号する。$M \equiv w^{-1} C$

$\equiv 702 \times 368195$

$\equiv 24149 \pmod{27481}$

ステップ０

$M_0 = 24149 / 1 = 24149$

$m_0 \equiv 24149 \times 1009^{-1} \equiv 6 \pmod{11}$

ステップ１

$M_1 = (24149 - 6 \times 1009) / 11 = 1645$

$m_1 \equiv 1645 \times 131^{-1} \equiv 7 \pmod{13}$

ステップ２

$M_2 = (1645 - 7 \times 131) / 13 = 56$

$m_2 = 56 / 7 = 8$

以上のようにして、メッセージｍ＝（６，７，８）を得る。

【００５１】（第３実施の形態）第２実施の形態では、基数ベクトル自体に乱数を組み込むようにしたが、第１実施の形態と同じ基数ベクトルを使用し、暗号文Ｃを作成する段階で乱数v_0，v_1，…，v_{K-1}を付加するようにすることもできる。この場合の暗号文Ｃは、第２実施の形態と同じ形となる。

【００５２】（第４実施の形態）第１実施の形態で基数ベクトルを多重化した第４実施の形態について説明する。第４実施の形態は、第１実施の形態による基数ベクトル｛B_i｝を２つの法それぞれにおいて設定し、中国人の剰余定理を利用した暗号化・復号方法である。この第４実施の形態でも、基数ベクトル｛B_i｝が超増加数列とはならず、ＬＬＬ法の攻撃に強い。また、平文の桁数を大きくできる。

【００５３】秘密鍵と公開鍵とを以下のように準備する。

・秘密鍵：｛b_{Pi}｝，｛b_{Qi}｝，Ｐ，Ｑ，Ｎ，ｗ

・公開鍵：｛c_i｝

２つの大きな素数Ｐ，Ｑを選択し、それらの積をＮとする。第１実施の形態におけるＫ個のb_iの集合を２通り準備し、｛b_{Pi}｝，｛b_{Qi}｝とする。また、それらより生成した基数を｛B_{Pi}｝，｛B_{Qi}｝とする。中国人の剰余定理を用いて、Ｐ，Ｑによる余りがそれぞれB_{Pi}，B_{Qi}となるような最小の整数B_iを導く。

【００５４】Ｎを法として、秘密の整数ｗを用いて、第１実施の形態と同様に、公開鍵ベクトルｃを以下の式（18），式（19）のように求める。

$$c_i \equiv w B_i \pmod N \quad \cdots (18)$$

$$c = (c_0, c_1, \cdots, c_{K-1}) \quad \cdots (19)$$

＊【００５５】メッセージベクトルｍと公開鍵ベクトルｃとの内積により、第１実施の形態と同様に（前記式（５））、暗号文Ｃを得る。

【００５６】復号処理は、以下のようにして行われる。暗号文Ｃに対して、法Ｐ，法Ｑにおいて、それぞれ中間復号文M_P，M_Qを式（20），式（21）のようにして求める。

$$M_P \equiv w^{-1}C \pmod P \quad \cdots (20)$$

$$M_Q \equiv w^{-1}C \pmod Q \quad \cdots (21)$$

【００５７】各中間復号文M_P，M_Qに関して、式（22），式（23）が成立する。

$$M_P = m_0 B_{P0} + m_1 B_{P1} + \cdots + m_{K-1} B_{PK-1} \quad \cdots (22)$$

$$M_Q = m_0 B_{Q0} + m_1 B_{Q1} + \cdots + m_{K-1} B_{QK-1} \quad \cdots (23)$$

【００５８】M_P，M_Qに対して、以下に示す逐次復号アルゴリズムIII を適用することによって、余りのペア（$m_i^{(P)}$，$m_i^{(Q)}$）を導くことができる。但し、m_iは、式（24），式（25）の何れかであるとする。

$$m_i \equiv m_i^{(P)} \pmod{b_{Pi+1}} \quad \cdots (24)$$

$$m_i \equiv m_i^{(Q)} \pmod{b_{Qi+1}} \quad \cdots (25)$$

これらに対して中国人の剰余定理を適用すると、メッセージ$m_i < lcm(b_{Pi+1}, b_{Qi+1})$を復号することができる。

【００５９】〔逐次復号アルゴリズムIII 〕

ステップ０

$M_{P0} = M_P / b_{P0}$

$M_{Q0} = M_Q / b_{Q0}$

$m_0^{(P)} \equiv M_{P0} \pmod{b_{P1}}$

$m_0^{(Q)} \equiv M_{Q0} \pmod{b_{Q1}}$

中国人の剰余定理によりm_0を求める。

ステップｉ（ｉ＝１～Ｋ－２）

$M_{Pi} = (M_{Pi-1} - m_{i-1}) / b_{Pi}$

$M_{Qi} = (M_{Qi-1} - m_{i-1}) / b_{Qi}$

$m_i^{(P)} \equiv M_{Pi} \pmod{b_{Pi+1}}$

$m_i^{(Q)} \equiv M_{Qi} \pmod{b_{Qi+1}}$

中国人の剰余定理によりm_iを求める。

ステップＫ－１

$m_{K-1} = (M_{PK-2} - m_{K-2}) / b_{PK-1}$

または

$m_{K-1} = (M_{QK-2} - m_{K-2}) / b_{QK-1}$

【００６０】ここで、第４実施の形態における具体例を示す。

・秘密鍵

$b_P = (1, 11, 19)$

$b_Q = (1, 13, 17)$

$B_P = (1, 11, 209)$

$B_Q = (1, 13, 221)$

$B = (1, 326859526, 1961157299)$

$P = 45053$

$Q = 54833$

$N = 2470391149$

$w = 320718294$

$w^{-1} \equiv 1798315174 \pmod N$

（B_P，B_Qでは超増加性が見られるが、Ｂは超増加数列ではない）

・公開鍵

$c \equiv wB$

$\equiv (320718294, 1521781250, 644798264) \pmod N$

・暗号化

メッセージをｍ＝（45，67，89）とする。

$C = c \cdot m$

$= 173778712476$

（メッセージの分割ビット数を11×13以下まで向上できる）

・復号

中間復号文M_P，M_Qを求め、逐次復号アルゴリズムIII を用いて復号する。

$M_P \equiv w^{-1}C \equiv 19383 \pmod{45053}$

$M_Q \equiv w^{-1}C \equiv 20585 \pmod{54833}$

ステップ０

$M_{P0} = 19383 / 1 = 19383$

$M_{Q0} = 20585 / 1 = 20585$

$m_{P0} \equiv 19383 \equiv 1 \pmod{11}$

$m_{Q0} \equiv 20585 \equiv 6 \pmod{13}$

$m_0 \equiv 45 \pmod{143}$

ステップ１

$M_{P1} = (19383 - 45) / 11 = 1758$

$M_{Q1} = (20585 - 45) / 13 = 1580$

$m_{P1} \equiv 1758 \equiv 10 \pmod{19}$

$m_{Q1} \equiv 1580 \equiv 16 \pmod{17}$

$m_1 \equiv 67 \pmod{323}$

ステップ２

$m_{P2} = (1758 - 67) / 19 = 89$

$m_{Q2} = (1580 - 67) / 17 = 89$

$m_2 = 89$

以上のようにして、メッセージｍ＝（45，67，89）を得

る。

【００６１】なお、合成数Ｎを法とする第４実施の形態のような多重化方式では、Ｎの素因数分解が困難である場合、Ｎを公開しても安全と考えられる。よって、そのような場合には、Ｎを法として求めた暗号文Ｃを送付することにより、暗号化効率が向上する。

【００６２】（第５実施の形態）第５実施の形態は、第４実施の形態に乱数を付加した暗号方式、言い換えると、第２実施の形態で基数ベタトルを多重化した暗号方式である。なお、この第５実施の形態については、前述の第１～第４実施の形態を参照すれば容易にその内容が理解されるので、詳細な説明は省略する。

【００６３】

【発明の効果】以上のように、本発明では、基数B_iを

$B_i = b_0, b_1 \cdots b_i$に設定するようにして、メッセージを多進法を用いて表現するようにしたので、高速な復号を行うことができる。この結果、積和型暗号の実用化の道を開くことに、本発明は大いに寄与できる。

【図面の簡単な説明】

【図１】２人のエンティティ間における情報の通信状態を示す模式図である。

【図２】本発明における復号の処理手順を示すフローチャートである。

【符号の説明】

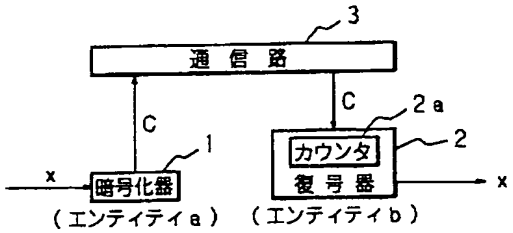
１　暗号化器

２　復号器

３　通信路

ａ，ｂ　エンティティ

【図１】



【図２】